

COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

“The DP World Controversy and the Ongoing Vulnerability of U.S. Seaports”

Written Testimony before

a hearing of the

Committee on Armed Services
United States House of Representatives

on

“The National Security Implications of the Dubai Ports World Deal to Take Over
Management of U.S. Ports”

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies
sflynn@cfr.org

Room 2118
Rayburn House Office Building
Washington, D.C.

1 p.m.
March 2, 2006

“The DP World Controversy and the Ongoing Vulnerability of U.S. Supports

by

Stephen E. Flynn

Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairman Hunter, Congressman Skelton, and distinguished members of the House Armed Services Committee. Thank you for inviting me this morning to discuss the DP World controversy and my assessment of where we are and where we need to be with regard to port security.

The controversy surrounding the takeover of five American container terminals by Dubai Ports World has had the salutary benefit of engaging Washington and the American people in a national conversation on the state of port security. This is long overdue given the enormous national security and economic security stakes should the next catastrophic terrorist attack on U.S. soil involve the global maritime transportation system and America’s waterfront.

My longstanding and deep concern about the persistent vulnerability of America’s homeland generally and the global supply chain and ports specifically is a matter of public record. This hearing represents the 16th time I have testified on these issues before the House and the Senate since September 11, 2001. On my first hearing on October 12, 2001 before the Senate Governmental Affairs Committee, I outlined the risk and consequences should a weapon of mass destruction be shipped to the United States in an intermodal container. Four years and four months later, my assessment is that the security measures that are currently in place do not provide an effective deterrent for a determined terrorist organization intent on exploiting or targeting the maritime transportation system to strike at the United States.

At the federal level, the primary frontline agencies—the Coast Guard and Customs and Border Protection Agency—are grossly under-funded for what became essentially a new major mission for them on 9/11. On the local and state levels, the size of port authority police forces remain tiny, providing often only token police presence within most seaports. Further, the U.S. government is still not organized to manage the aftermath of an attack involving our seaports which will translate into unnecessary loss of life, profound economic disruption, and a serious loss of public confidence.

Should terrorists strike in a major U.S. seaport tomorrow, Americans will experience a post-Katrina sense of dismay and frustration at how little the federal government has been investing to effectively safeguard this critical national and economic security asset.

With those sobering words in mind, it may come as a surprise to many that my assessment of the national security implications of the DP World purchase of Peninsular and Orient Navigations systems and the leases to five containers terminals on the East Coast and New Orleans is that this commercial transaction will not *qualitatively* effect the overall state of global and American maritime transportation security. Stated

differently, should a U.S. company assume control of these terminal operations tomorrow, it would not qualitatively improve our security. This is because the problem is less about who owns and operates U.S. container terminals than it is that we simply have not addressed far more serious supply chain, maritime, and port security issues that would dramatically reduce the terrorist risk to our homeland.

This is not to say that it is necessary and appropriate to closely examine the national security implications of this agreement or that of any transaction that involves a foreign government having an ownership interest in critical U.S. assets. Further, based on research I have done on the broader issue of critical infrastructure protection and homeland security, I believe the criteria used in the CFIUS process is sorely in need of reexamination given the transformation in warfare that is elevating the likelihood and consequences of asymmetric attacks on economic targets. However, the nature of confronting the risk to our seaports necessarily requires a global approach and a closely partnering with the largely foreign-owned companies who own and operate the overwhelming majority of the ships, terminals, and logistics companies that connect the U.S. economy to the world. Accordingly, if DP World receives a clean security bill-of-health after the 45-day review process, it is important that we reach out to the company to make it a part of global container security solution.

To put this current controversy into a broader security context, let me share with you the terrorist scenario that most keeps me awake at night, and why I spend most of my days trying to convey a greater sense of urgency and why I have been working to design and promote meaningful measures to address this issue.

Based on my experience and research on this issue for nearly 15 years, I believe that the greatest vulnerability that will involve the maritime sector and our seaports is overseas within the transportation system before a container reaches a loading port. Specifically, the biggest security gap is in the transportation system once a container leave the factory. This is for three reasons. First, the local truck drivers are typically poorly paid and often belong to very small firms operating on very thin profit margins. Second, there are no mandated standards for seals or locks on containers. Most are lead numbered straps that pass through the pad-eye of the doors. Some are mechanical seals that typically cost \$1. And as experienced investigators of cargo thieves and smugglers know, criminals have long ago determined how to gain access to a container without even tampering with the seal. Third, these containers travel through often remote and at times dangerous jurisdictions.

So here's a plausible scenario informed by insights provided to me by Gary Gilbert, the Chairman of the Corporate Security Council and Senior Vice President for Hutchison Port Holdings (HPH). HPH is the largest container terminal operator in the world, operating in 42 ports and moving nearly 50 million containers in 2005.

A container of athletic foot wear for a name brand company is loaded at a manufacturing plant in Surabaya, Indonesia. The container doors are shut and a mechanical seal is put into the door pad-eyes. These designer sneakers are destined for retail stores in malls

across America. The container and seal numbers are recorded at the factory. A local truck driver, sympathetic to al Qaeda picks up the container. On the way to the port, he turns into an alleyway and backs up the truck at a nondescript warehouse where a small team of operatives pry loose one of the door hinges to open the container so that they can gain access to the shipment. Some of the sneakers are removed and in their place, the operatives load a dirty bomb wrapped in lead shielding, and they then refasten the door.

The driver takes the container now loaded with a dirty bomb to the port of Surabaya where it is loaded on a coastal feeder ship carrying about 300 containers for the voyage to Jakarta. In Jakarta, the container is transferred to an Inter-Asia ship which typically carry 1200-1500 containers to the port of Singapore or the Port of Hong Kong. In this case, the ship goes to Hong Kong where it is loaded on a super-container ship that carries 5000-8000 containers for the trans-Pacific voyage. The container is then off-loaded in Vancouver, British Columbia. Because it originates from a trusted-name brand company that has joined the Customs-Trade Partnership Against Terror, the shipment is never identified for inspection by the Container Security Initiative team of U.S. customs inspectors located in Vancouver. Consequently, the container is loaded directly from the ship to a Canadian Pacific railcar where it is shipped to a railyard in Chicago. Because the dirty bomb is shielded in lead, the radiation portals currently deployed along the U.S.-Canadian border do not detect it. When the container reaches a distribution center in the Chicago-area, a triggering device attached to the door sets the bomb off.

There would be four immediate consequences associated with this attack. First, there would be the local deaths and injuries associated with the blast of the conventional explosives. Second, there would be the environmental damage done by the spread of industrial-grade radioactive material. Third, there would be no way to determine where the compromise to security took place so the entire supply chain and all the transportation nodes and providers must be presumed to present a risk of a potential follow-on attack. Fourth—and perhaps most importantly—all the current container and port security initiatives would be compromised by the incident.

In this scenario, the container originated from one of the 5,800 companies that now belong to the Customs-Trade Partnership Against Terrorism. It would have transited through multiple ports—Surabaya, Jakarta, Hong Kong, and Vancouver—that have been certified by their host nation as compliant with the post-9/11 International Ship and Port Facility Security (ISPS) Code that came into effect on 1 July 2004. Because it came from a trusted shipper, it would not have been identified for special screening by the Container Security Initiative team of inspectors in Hong Kong or Vancouver. Nor would it have been identified by the radiation portal. As a consequence, governors, mayors, and the American people would have no faith in the entire risk-management regime erected by the administration since 9/11. There will be overwhelming political pressure to move from a 5 percent inspection rate to a 100 percent inspection rate, effectively shutting down the flow of commerce at and within our borders. Within two weeks, the reverberations would be global. As John Meredith, the Group Managing Director of Hutchison Port Holdings, warned in a Jan 20, 2004 letter to Robert Bonner, the former

Commissioner of the U.S. Customs and Border Protection: “. . . **I think the economic consequences could well spawn a global recession – or worse.**”

In short the stakes are enormous. But there are four factors associated with the scenario that I just laid out that usefully informs the focus of this hearing. First, the threat is not so much tied to seaports as it is global supply chains that now large operate largely on an honor system because the standards are so nominal and the capacity for agencies like the Coast Guard and customs is negligible. Second, no container terminal operator within the United States or abroad really know what are in the containers that pass through their facilities. They are in the business of receiving and discharging them from and to ships, trucks, and trains that converge at their terminals as quickly, reliably, and at the lowest cost possible. Third, as the engagement of John Meredith and Gary Gilbert of HPH on this issue reflects (HPH has no terminals inside the United States) global terminal operators are deeply concerned about the terrorist threat involving or directed at the supply chain because their billions of dollars of investment tied up in worldwide infrastructure are at risk. Four, the scenario I just laid out involved Vancouver as the offload port in North America, highlighting that the challenge of managing this threat is far greater than bolstering the physical security measures of U.S. seaports.

This story also highlights that there can be no solution unless U.S. authorities work directly with overseas terminal operators in enlisting their help to manage the problem. This is the case I posited in a February 28, 2006 New York Times op-ed article with Admiral James Loy, the former Deputy Secretary of Homeland Security and former Administrator of the Transportation Security Administration, and the former Commandant of the Coast Guard. We point out that ports are the on- and offramps to global markets, and they belong to a worldwide system operated by many different private and public entities. A major step in that direction would be to construct a comprehensive global container inspection system that scans the contents of every single container destined for America's waterfront before it leaves a loading port — rather than scanning just the tiny percentage we do now, after they have already arrived within a seaport.

The model for this recommendation is a pilot project that has been underway in the Port of Hong Kong since January 2005. There every container entering the truck gates of two of the world's busiest container terminals has passed through scanning and radiation detection devices. Images of the containers' contents are then stored on computers so that they could be scrutinized remotely by American or other customs authorities almost in real time. Customs inspectors can then issue orders not to load a container that worries them. Since this system involves scanning every container and not just those destined for the United States, it would help to support international counter-proliferation efforts as well.

In the view of Admiral Jim Loy and I, the Dubai deal provides an opportunity to adopt a system like the one in Hong Kong globally. The White House and Customs should embrace Dubai Ports World's offer to provide additional guarantees to protect the five American terminals it wants to run. The company should agree to install scanning and

radiation detection equipment at the entry gates of its terminals in the Middle East, Europe, Asia, North America and South America within the next two years.

By making this commitment, the company could address head-on the anxiety about this transaction that has led to this hearing within the Congress that is fueling the uproar around the country. Instead of a 5 percent inspection solution we are currently using, we could move towards a 100 percent solution. The 45-day review period that has recently been agreed upon should provide the breathing room to work out the details. Congress and the White House should appropriate the necessary funds within the FY07 appropriation cycle to insure that the Customs and Border Protection agency has the staffing and information systems upgrades to tap the revolutionary potential of such a comprehensive inspection approach.

Hutchison Port Holdings would probably join Dubai Ports World in putting Hong Kong-style inspection systems in place within its 42 ports around the world. Hutchison's chief executive, John Meredith, is an outspoken advocate for improving container security and has championed the Hong Kong pilot program, which runs in one of its terminals. His enthusiasm for the project is shared by Sean Kelly, a U.S. citizen who is currently the Managing Director of Modern Terminals in Hong Kong where the second pilot has been running.

Hutchison Port Holdings along with PSA Singapore Terminals, Dubai Ports World and Denmark's APM Terminals handle nearly eight out of every 10 containers destined for the United States. If they agreed to impose a common security fee of roughly \$20 per container, similar to what passengers are now used to paying when they purchase airline tickets, they could recover the cost of installing and operating this system worldwide. This, in turn, would furnish a powerful deterrent for terrorists who might be tempted to convert the ubiquitous cargo container into a poor man's missile.

This global regime for container security will require oversight. Congress should require that the security plans developed by importers under the Customs-Trade Partnership Against Terrorist (C-TPAT) be independently audited. It should also provide the Department of Homeland Security with adequate Customs and Coast Guard inspectors to audit these auditors. Today Customs has only 80 inspectors to monitor the compliance of the 5,800 importers who have vowed to secure their goods as they travel from factories to ship terminals. To assess worldwide compliance with the International Ship and Port Facility Security Code, the Coast Guard has just 20 inspectors — roughly the size of the average passenger screening team at an airport security checkpoint.

The administration and Congress should also support the development and deployment of technologies that can monitor the position and integrity of shipments as they move through the global supply chain. There are a number of technologies that draw on low-orbit satellites and radio-frequency identification systems that have promise in this regard. The widespread deployment of these technologies can have the ancillary commercial benefits as well by improving global logistics management by bolstering supply chain visibility and accountability.

At the end of the day, America's port security challenge is not about who is operating on our waterfront. The real issue is that we are relying on commercial companies largely to police themselves with nominal standards and very limited oversight. Both Congress and the White House should embrace a framework of "trust but verify," in President Ronald Reagan's phrase, based on real standards and real oversight. When it comes to the flow of goods around the planet, we need to know what's in the box more than we need to know who is moving them around a container yard.

The bottom line is that if at the end of this controversy, the only thing that happens is that the Dubai Port World deal is approved or denied, the American people will have been deprived of a real opportunity to have advanced a qualitative improvement in port and container security. Congress and the White House should work together to convert the current political maelstrom into doing something meaningful to bolster our national security and economic security.

Thank you and I look forward to responding to your questions.

Stephen Flynn is the author of the critically acclaimed and national bestseller, *America the Vulnerable*. He is currently writing a new book to be published by Random House in Fall 2006 entitled, *The Edge of Disaster: Catastrophic Storms, Terror, and American Recklessness*. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report “*America: Still Unprepared—Still in Danger*,” co-chaired by former Senators Gary Hart and Warren Rudman. Since 9/11 he has provided congressional testimony on homeland security matters on fifteen occasions. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issues on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.

]